IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Mehrban Jam	§	Art Unit:	2162
Serial No.:	09/836,952	§		
		§	Examiner:	Fred I. Ehichioya
Filed:	April 17, 2001	§		
For:	System and Method for Providing Context-Aware Computer Management Using Smart Identification Badges	§	Atty. Dkt. No.:	10005248-1 (HPC.0209US)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF PURSUANT TO 37 C.F.R § 41.37

Sir:

The final rejection of claims 1-38 is hereby appealed.

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF THE CLAIMS

Claims 1-38 have been finally rejected and are the subject of this appeal.

Date of Deposit: March 12, 2008

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent Office on the date indicated above.

Ginger Yount

Ginger Yount

IV. STATUS OF AMENDMENTS

No amendment after final rejection has been submitted.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

Independent claim 1 recites a computer-implemented method comprising:

assigning information stored on a computer (Fig. 2:202) a plurality of clearance levels (Spec., 8:9-20);

assigning each smart badge (Fig. 2:210, 212, 214, 216) within a set of smart badges a corresponding one of the clearance levels (Spec., 8:10-11);

using a wireless beacon (Fig. 2:206) to detect which smart badges are located within a predefined boundary (Spec., 8:5-8);

identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary (Spec., 9:16-10:12); and

providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level (Spec., 9:16-10:12).

Independent claim 12 recites a method for context-aware computer management comprising:

assigning database information a plurality of clearance levels (Spec., 8:9-20);

assigning each smart badge within a set of smart badges a corresponding one of the clearance levels (Spec., 8:10-11);

using a wireless beacon (Fig. 2:206) to detect which smart badges are located within a predefined physical boundary (Spec., 8:5-8);

identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary (Spec., 9:16-10:12);

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (Spec., 9:16-10:12);

defining those smart badges within the boundary as a set of visible smart badges (Spec., 11:5-7);

updating the set of visible smart badges in response to a change in smart badge visibility status (Spec., 11:8-13:4); and

recalculating the lowest clearance level in response to the change in smart badge visibility status (Spec., 9:16-10:12).

Independent claim 13 recites a computer-usable medium embodying computer program code that when executed by a computer causes performance of context-aware computer management, comprising:

assigning database information a plurality of clearance levels (Spec., 8:9-20);

assigning each smart badge within a set of smart badges a corresponding one of the clearance levels (Spec., 8:10-11);

using a wireless beacon (Fig. 2:206) to detect which smart badges are located within a predefined physical boundary (Spec., 8:5-8);

identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary (Spec., 9:16-10:12); and

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (Spec., 9:16-10:12).

Independent claim 20 recites a system for context-aware computer management comprising:

means for assigning database information a plurality of clearance levels (Spec., 8:9-20);

means for assigning each smart badge within a set of smart badges a corresponding one of the clearance levels (Spec., 8:10-11);

means for using a wireless beacon (Fig. 2:206) to detect which smart badges are located within a predefined physical boundary (Spec., 8:5-8);

means for identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary (Spec., 9:16-10:12);

means for providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (Spec., 9:16-10:12);

means for defining those smart badges within the boundary as a set of visible smart badges (Spec., 11:5-7);

means for updating the set of visible smart badges in response to a change in smart badge visibility status (Spec., 11:8-13:4); and

means for recalculating the lowest clearance level in response to the change in smart badge visibility status (Spec., 9:16-10:12).

Independent claim 21 recites a system for context-aware computer management comprising:

a database (Fig. 2:208), including information differentiated by a plurality of clearance levels (Spec., 8:9-20);

a first wireless beacon (Fig. 2:206);

a set of smart badges (Fig. 2:210, 212, 214, 216), detected by the first wireless beaeon to be within a predefined boundary, each badge assigned a corresponding one of the clearance levels (Spec., 8:5-8, 10-11);

a computer (Fig. 2:202) located within the boundary (Spec., 7:3-7);

a system service module (Fig. 2:218), coupled to the first wireless beacon, for identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary (Spec., 9:6-10:12); and

a software application (Fig. 2:222), coupled to the system service module and the database, for providing access to that sub-set of the information within the database having a clearance level no higher than the lowest identified clearance level on the computer (Spec., 9:6-10:12).

Independent claim 31 recites a computer-usable medium containing program code that when executed cause a computer to:

store plural sub-sets of information, each sub-set of information associated with one of plural clearance levels (Spec., 8:9-20);

use at least a first wireless beacon (Fig. 2:206) to communicate with plural badges (Fig. 2:210, 212, 214, 216) within a predefined region, each of the plural badges associated with one of the plural clearance levels (Spec., 8:5-8);

determine a lowest clearance level from among the clearance levels associated with the badges in the predefined region (Spec., 9:16-10:12); and

provide access to one or more sub-sets of the information having one or more respective clearance levels no higher than the determined lowest clearance level (Spec., 9:16-10:12).

Independent claim 36 recites a system comprising:

storage to store sub-sets of information associated with corresponding plural clearance levels (Spec., 8:9-20);

a first wireless beacon (Fig. 2:206) to communicate wirelessly with badges (Fig. 2:210, 212, 214, 216) within a predefined region, each of the badges associated with one of the plural clearance levels (Spec., 8:5-8);

a module (Fig. 2:218) to identify a lowest clearance level from among the clearance levels of the badges within the predefined region (Spec., 9:6-10:12); and

software (Fig. 2:222) to provide access to one or more sub-sets of information in the storage having one or more clearance levels no higher than the identified lowest clearance level (Spec., 9:6-10:12).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-38 Rejected Under 35 U.S.C. § 102(e) As Anticipated By Non-Patent Literature, "WIPS Technical Documentation," by Roland Ljungh et al. (Ljungh).

VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-headings as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Claims 1-38 Rejected Under 35 U.S.C. § 102(e) As Anticipated By Non-Patent Literature, "WIPS Technical Documentation," by Roland Ljungh et al. (Ljungh).

1. Claims 1-8, 11, 13-17, 21-28, 31-33, 35, 36.

The Examiner has erred in rejecting claim 1 as being anticipated by Ljungh.

Claim 1 recites, *inter alia*, identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary, and providing access to that sub-set of the information (stored on a computer) having a clearance level no higher than the lowest identified clearance level.

As disclosing these two elements of claim 1, the Examiner cited page 16, § 4.2.8 of Ljungh (as corresponding to the identifying element of claim 1) and pages 6, 7, and 15, § 4.2.1 of Ljungh (as corresponding to the providing element of claim 1). 11/15/2007 Office Action at 5.

Section 4.2.8 of Ljungh refers to a guest badge that is the same as an ordinary badge other than in appearance and lower priority levels regarding access to certain areas. Other than reference to a guest badge and the fact that a guest badge has lower priority levels regarding access to certain areas, there is no teaching provided in § 4.2.8 of Ljungh of "identifying a lowest

clearance level from among the clearance levels assigned to the smart badges within the boundary." This is a first point of error made by the Examiner.

Section 4.2.1 on page 15 of Ljungh refers to door opening features using the badges described in Ljungh. This section of Ljungh refers to the desire for automatic door opening that uses badge authentication. The passage also refers to verifying that the badge is in the possession of its owner by using a voice sensor on the badge for authentication through voice identification. The passage also notes that as the badge owner approaches the door in question, the badge receives a challenge question from an IR transceiver positioned at the door, and the owner must authenticate himself within a certain time to grant the owner access through the door.

However, there is no teaching in § 4.2.1 of Ljungh of providing access to that sub-set of information having a clearance level no higher than the *lowest identified clearance level* (which was identified from among the clearance levels assigned to the smart badges within the boundary). All § 4.2.1 of Ljungh teaches is automatic door opening based on voice authentication – there is no teaching of providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level.

In the citation of § 4.2.1 of Ljungh, the Examiner referred to access in Ljungh being "given in accordance with different security levels." Although that discussion does not appear in § 4.2.1 of Ljungh, it is noted that § 4.1.1 of Ljungh refers to a security system with "different levels of access" that can be configured by the users themselves. However, the reference to the security system with different levels of access is completely un-related to the subject matter recited in claim 1, which refers to identifying a lowest clearance level from among the clearance levels assigned to smart badges within the boundary (as detected by a wireless beacon), and

providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level.

The citation of pages 6 and 7 of Ljungh is also unavailing. Page 6 of Ljungh refers to a database table that contains information about user name, password, real name, present room, and when the location of a person was last reported. Page 6 of Ljungh also notes that this table contains information about which badge the person is wearing and the IP address of his or her laptop computer.

Page 7 of Ljungh provides a discussion of a database server. In particular, the Examiner referred to the passage in Ljungh regarding the database server having methods for finding out whether or not a particular user is allowed to see and update certain information in the database. However, this teaching of Ljungh is still different from the subject matter of claim 1. Note that claim 1 specifically recites identifying a **lowest clearance level** from among a plurality of clearance levels assigned to smart badges within a boundary, in combination with providing access to that sub-set of the information having a clearance level no higher than the **lowest identified clearance level**. The concept of identifying a **lowest** clearance level and then providing access to that sub-set of information having a clearance level no higher than the **lowest** identified clearance level is clearly not taught by Ljungh. The passage on page 7 of Ljungh refers to finding whether or not a **particular** user is allowed to see certain information in the database – there is absolutely nothing here to even hint at identifying a **lowest** clearance level from among a plurality of clearance levels assigned to smart badges within a boundary, and then providing the access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level.

In view of the foregoing, it is clear that claim 1 and its dependent claims are not anticipated by Ljungh.

Independent claims 13, 21, 31, and 36 and their respective dependent claims are allowable over Ljungh for similar reasons as those stated above with respect to claim 1.

In view of the foregoing, reversal of the final rejection of the above claims is respectfully requested.

2. Claims 9, 18, 34.

Claims 9, 18, and 34 depend from independent claims 1, 13, and 31, respectively, and therefore are allowable for at least the same reasons as the corresponding base claims. Moreover, claim 9 recites defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers.

The Examiner cited page 15, § 4.2.1, ¶ 1, of Ljungh as disclosing this subject matter. The cited passage refers to door opening features, in which detecting whether a badge has been stolen or falsified can be accomplished by using a voice sensor on the badge for authentication through voice identification. Voice identification to authenticate a user is different from what is recited in claim 9, which is defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers. The subject matter of the claim is nowhere hinted at by Ljungh.

This is a further reason that claim 9 is not anticipated by Ljungh.

Claims 18 and 34 are similarly allowable over Ljungb.

Reversal of the final rejection of the above claims is respectfully requested.

3. Claims 10, 19.

Claims 10 and 19 depend from claims 1 and 13, and therefore, are allowable for at least the same reasons as the corresponding base claims.

Moreover, dependent claim 10 recites assigning an expiration period to each of the smart badges, and de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded. With respect to the expiration period, the Examiner cited page 9, first paragraph, of Ljungh, which refers to a thread at a badge server serving a specific badge until the badge either closes the connection or a timeout occurs. 11/15/2007 Office Action at 8. The Examiner stated that the timeout is interpreted as being the expiration period of claim 10. *Id.* With respect to the de-authenticating and erasing clause, the Examiner cited page 14, § 4.1.5, second paragraph, of Ljungh, which refers to use of an administration tool to remove data. However, the removal of data as performed in § 4.1.5 of Ljungh is *not* based on the expiration period (timeout noted on page 9 of Ljungh) having being exceeded. Therefore, claim 10 is not anticipated by Ljungh for this additional reason.

Claim 19 is similarly further allowable over Ljungh.

Reversal of the final rejection of the above claims is respectfully requested.

4. Claims 29, 30, 37, 38.

Claims 29, 30, 37, and 38 depend from independent claims 1 and 36, respectively, and are therefore not anticipated by Ljungh for at least the same reasons as claims 1 and 36.

Claim 29 further recites the use of a first wireless beacon and a second wireless beacon, where detecting which smart badges are located within the predefined boundary is based on the first and second wireless beacons, and where the second wireless beacon is able to communicate

with smart badges outside the predefined boundary, and the first wireless beacon is blocked from communicating with smart badges outside the predefined boundary.

The Examiner cited page 17 of Ljungh as disclosing the use of RF receivers/transmitters. A stated drawback of RF is that RF signals travel through walls. However, note that the radio technology described in § A.2 of Ljungh is proposed as an *alternative* to the IR technology. Therefore, it is clear that Ljungh does not disclose the use of both IR and RF beacons for the purpose of detecting which smart badges are located within the predefined boundary.

Claim 29, and its dependent claim, are thus further allowable for the above reasons.

Claim 37, and its dependent claim, are also further allowable for similar reasons as claim 29.

Reversal of the final rejection of the above claims is respectfully requested.

5. Claims 12, 20.

Independent claim 12 is also not anticipated by Ljungh. More specifically, claim 12 recites identifying a lowest clearance level from among a plurality of clearance levels (assigned to the smart badges within the houndary), and providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary.

As discussed above with respect to claim 1, Ljungh does not provide any teaching of this subject matter of claim 12.

Moreover, claim 12 also recites recalculating the lowest clearance level in response to the change in smart badge visibility status. As discussed, the concept of a lowest clearance level is clearly not present in Ljungh. Therefore, the concept of recalculating the lowest clearance level would also not be taught by Ljungh.

Therefore, claim 12 is not anticipated by Ljungh.

Independent claim 20 is similarly allowable over Ljungh.

Reversal of the final rejection of the above claims is respectfully requested.

CONCLUSION

In view of the foregoing, reversal of all final rejections and allowance of all pending claims is respectfully requested.

Respectfully submitted,

Date: 3/12/2008

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

VIII. APPENDIX OF APPEALED CLAIMS

The claims on appeal are:

1. A computer-implemented method comprising:

assigning information stored on a computer a plurality of clearance levels;

assigning each smart badge within a set of smart badges a corresponding one of the clearance levels;

using a wireless beacon to detect which smart badges are located within a predefined boundary;

identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary; and

providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level.

2. The method of claim 1 further comprising:

defining those smart badges within the boundary as a set of visible smart badges; and

updating the set of visible smart badges in response to a change in smart badge visibility status.

3. The method of claim 2 further comprising:

recalculating the lowest clearance level in response to the change in smart badge visibility status.

4. The method of claim 2 further comprising:

recording the smart badge visibility status of each smart badge within an activity log.

5. The method of claim 1 wherein providing includes:

providing access to smart badge wearers assigned to the smart badges.

6. The method of claim 2 further comprising:

preventing access to the information when the smart badge visibility status is set to invisible for a predetermined timeout.

7. The method of claim 1 further comprising:

writing data items to the smart badges.

8. The method of claim 7 further comprising:

pre-reading the data items from the smart badges during idle periods.

9. The method of claim 1 further comprising

defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers.

10. The method of claim 1 further comprising:

assigning an expiration period to each of the smart badges; and

de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded.

11. The method of claim 1 wherein the using element includes:

configuring the predefined boundary by varying a sensitivity level of the wireless beacon.

12. A method for context-aware computer management comprising:

assigning database information a plurality of clearance levels;

assigning each smart badge within a set of smart badges a corresponding one of the clearance levels;

using a wireless beacon to detect which smart badges are located within a predefined physical boundary;

identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary;

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary;

defining those smart badges within the boundary as a set of visible smart badges;

updating the set of visible smart badges in response to a change in smart badge visibility status; and

recalculating the lowest clearance level in response to the change in smart badge visibility status.

13. A computer-usable medium embodying computer program code that when executed by a computer causes performance of context-aware computer management, comprising:

assigning database information a plurality of clearance levels;

assigning each smart badge within a set of smart badges a corresponding one of the clearance levels;

using a wireless beacon to detect which smart badges are located within a predefined physical boundary;

identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary; and

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary.

14. The computer-usable medium of claim 13 wherein the context-aware computer management further comprises:

defining those smart badges within the boundary as a set of visible smart badges; and

updating the set of visible smart badges in response to a change in smart badge visibility status.

15. The computer-usable medium of claim 14 wherein the context-aware computer management further comprises:

recalculating the lowest clearance level in response to the change in smart badge visibility status.

16. The computer-usable medium of claim 13 wherein providing includes:

providing access to the database information to smart badge wearers assigned to the smart badges.

17. The computer-usable medium of claim 14 wherein the context-aware computer management further comprises:

preventing access to the database when the smart badge visibility status is set to invisible for a predetermined timeout.

18. The computer-usable medium of claim 13 wherein the context-aware computer management further comprises:

defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers.

19. The computer-usable medium of claim 13 wherein the context-aware computer management further comprises:

assigning an expiration period to each of the smart badges; and

de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded.

20. A system for context-aware computer management comprising:

means for assigning database information a plurality of clearance levels;

means for assigning each smart badge within a set of smart badges a corresponding one of the clearance levels;

means for using a wireless beacon to detect which smart badges are located within a predefined physical boundary;

means for identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary;

means for providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary;

means for defining those smart badges within the boundary as a set of visible smart badges;

means for updating the set of visible smart badges in response to a change in smart badge visibility status; and

means for recalculating the lowest clearance level in response to the change in smart badge visibility status.

21. A system for context-aware computer management comprising:

a database, including information differentiated by a plurality of clearance levels;

a first wireless beacon;

a set of smart badges, detected by the first wireless beacon to be within a predefined boundary, each badge assigned a corresponding one of the clearance levels;

a computer located within the boundary;

a system service module, coupled to the first wireless beacon, for identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary; and

a software application, coupled to the system service module and the database, for providing access to that sub-set of the information within the database having a clearance level no higher than the lowest identified clearance level on the computer.

22. The system of claim 21, wherein the first beacon includes:
a wide angle RF beacon.

23. The system of claim 21, further comprising:
a second diffuse IR beacon, coupled to the service module, limited to detecting smart badges within the predefined boundary.

24. The system of claim 21, wherein the smart badges include:
biometric sensors for detecting when a smart badge has been removed from an assigned smart badge wearer.

25. The system of claim 21, wherein the service module
defines those smart badges within the boundary as a set of visible smart badges, and
recalculates the lowest clearance level in response to a change in a visibility status.

26. The system of claim 21, wherein the application logs smart badge wearers assigned to visible smart badges onto the computer.

27. The method of claim 1, wherein providing access to the sub-set of information comprises providing access to the sub-set of information stored on the computer located within the predefined boundary.

28. The method of claim 1, wherein the wireless beacon comprises a first wireless beacon to communicate with the smart badges, the method further comprising:
using a second wireless beacon to communicate with the smart badges,
wherein detecting which smart badges are located within the predefined boundary is based on the first and second wireless beacons.

29. The method of claim 28, wherein using the second wireless beacon comprises using the second wireless beacon to eommunicate with smart badges within the predefined boundary and to communicate with smart badges outside the predefined boundary through one or more blocking objects defining the predefined boundary, and

using the first wireless beacon comprises using the first wireless beacon to communicate with smart badges within the predefined boundary, wherein the first wireless beacon is blocked from communicating with smart badges outside the predefined boundary by the one or more blocking objects.

30. The method of claim 29, wherein using the first wireless beacon comprises using an infrared beacon, and wherein using the second wireless beacon comprises using a radio frequency beacon.

31. A computer-usable medium eontaining program code that when executed cause a computer to:

store plural sub-sets of information, each sub-set of information associated with one of plural clearance levels;

use at least a first wireless beacon to communicate with plural badges within a predefined region, each of the plural badges associated with one of the plural clearance levels;

determine a lowest clearance level from among the clearance levels associated with the badges in the predefined region; and

provide access to one or more sub-sets of the information having one or more respective clearance levels no higher than the determined lowest clearance level.

32. The computer-usable medium of claim 31, wherein providing access to the one or more sub-sets of the information comprises displaying the one or more sub-sets of the information having the one or more respective clearance levels no higher than the determined lowest clearance level.

33. The computer-usable medium of claim 31, wherein the program code when executed cause the computer to further:

use a second wireless beacon to communicate with the plural badges in the predefined region and to communicate with one or more badges outside the predefined region,

wherein the first wireless beacon is able to communicate with the plural badges within the predefined region but is unable to communicate with the one or more badges outside the predefined region; and

determining the badges that are within the predefined region based on the first and second wireless beacons.

34. The computer-usable medium of claim 31, wherein the program code when executed cause the computer to further:

receive a parameter from each of the badges, the parameter indicating a confidence level that the respective badge has been worn continuously by a user.

35. The computer-usable medium of claim 31, wherein the program code when executed cause the computer to further:

re-determine the lowest clearance level as badges enter or leave the predefined region.

36. A system comprising:

storage to store sub-sets of information associated with corresponding plural clearance levels;

a first wireless beacon to communicate wirelessly with badges within a predefined region, each of the badges associated with one of the plural clearance levels;

a module to identify a lowest clearance level from among the clearance levels of the badges within the predefined region; and

software to provide access to one or more sub-sets of information in the storage having one or more clearance levels no higher than the identified lowest clearance level.

37. The system of claim 36, further comprising:

a second wireless beacon to communicate wirelessly with badges within the predefined region and at least one badge outside the predefined region,

wherein the first wireless beacon is unable to communicate with the at least one badge outside the predefined region,

the module to detect the badges that are within the predefined region based on the first and second wireless beacons.

38. The system of claim 37, wherein the second wireless beacon comprises a radio frequency beacon, and the first wireless beacon comprises an infrared beacon.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.